大学の情報システムを認証から俯瞰する：情報サービスを「こわれもの」にしないために

AUTHOR(S):

上田, 浩

大学の情報システムを認証から俯瞰する：情報サービスを「こわれもの」にしないために

京都大学 学術情報メディアセンター 上田 浩 *

概要

本稿では，筆者が大学の情報サービスにインフラからコンテンツまでかかわってきた経験をもとに，「認証基盤を制する者が大学の情報システムを制する」という知見を，その構築運用事例を通して主張する．具体的には，群馬大学における，ネットスプリング社 AXIOLE，アルカテル・ルーセント社 OmniSwitch/OmniAccess を採用した認証の統合プロジェクト，京都大学における Microsoft クラウドサービスの統合認証システムとの Shibboleth 連携事例を総括する．群馬大学における統一認証基盤の整備により，大学情報データベース，マイクロソフト包括ライセンス，VPN 接続サービス，802.11n 無線 LAN，光直収ネットワークにおける MAC アドレス認証 VLAN など魅力的なサービスを提供することができた．一方，京都大学における Microsoft Office365 の Shibboleth 認証連携については費したリソースにもかかわらず，様々な不具合が露呈した．我々のパブリッククラウドのリスク認識が甘かったことは否めないが，Microsoft のクラウド側ソフトウェア，システム運用，サポート体制には改善の余地がある．これらの事例は，認証基盤の整備はキラーアプリケーションと一体で進めなければならないこと，クラウドサービスは認証基盤普及のキラーアプリになり得るが，諸刃の剣でもあることを示している．情報システムはその構築コストゆえに，目的に合わせ最適化されるという特性があり，認証基盤も例外ではない．情報システムを「こわれもの」にしないためには，キラーアプリケーションの充実のための認証基盤の定期的なスクラップ・アンド・ビルドを行うか，十年先を見据えた拡張性の高いシステム設計が今後の課題となるであろう．

1 はじめに

大学の学内 LAN，情報システムの歴史は企業のそれより古く，歴史的経緯を引きずった運用がなされている場合が少なくない．たとえば，キャンパスごとに認証基盤が別個に存在して学生をはじめとする利用者の利便性が低くなっていたり，適切なアクセス制御が困難であったりする．この根底にあるのは大学という組織が，減点主義と言われる公務員の体質と，個人商店とも揶揄される独立性の高い教員の集まりであることが指摘される．

2000 年代前半から，大学における認証の統合の必要性が認識され，先進的な取り組みが報告されてきた [1, 2, 3]．これらの取り組みを始めとして，大学における認証基盤の統合は進んできたものの，学内 LAN を認証 LAN として運用することは各大学のリソースの問題，誰を利用者とするかという大学構成員の定義の問題，高いとは言えない情報セキュリティ意識に加え，前述した大学組織の特性上，トップダウンで物事を進めることが困難であること，大学の自治を尊重するという形式的風潮から進んでいない [4, 5]．加えて近年，情報システムの可用性向上と運用コスト削減のため学内サービスをクラウドサービス利用によるものとすることが一般的になっているが，認証連携にはそれなりのコストが必要となる．そのため，認証の統合という流れを継続し認証連携するのが良いのか，クラウドはクラウドとして As Is で利用するのかという問題に関し決め手となるような，大学間の情報共有が進んでいるとは言い難い．

本稿は，筆者が大学の情報サービスにインフラからコンテンツまでかかわってきた経験をもとに，「認証基盤を制する者が大学の情報システムを制す

* @UEDA_Hiroshi, uep@media.kyoto-u.ac.jp

る」という知見を主張するものである．具体的な事例として，群馬大学における認証の統合プロジェクト，京都大学におけるクラウドサービスの統合認証システムとの Shibboleth 連携を総括する．前者においては統一認証基盤の整備により，大学情報データベース，マイクロソフト包括ライセンス，VPN 接続サービス，802.11 無線 LAN，MAC アドレス認証 VLAN など魅力的なサービスを提供することができた．一方後者においては，費したリソースにもかかわらず，様々な不具合が露呈した．我々のパブリッククラウドのリスク認識が甘かったことは否めないが，Microsoft のクラウド側ソフトウェア，システム運用，サポート体制には改善の余地がある．これらの事例を通し，認証基盤の整備はキラーアプリケーションと一体で進めなければならないこと，クラウドサービスは認証基盤普及のキラーアプリになり得るが，諸刃の剣でもあることを述べる．

以下，2 節で群馬大学の認証の統合プロジェクトについて，3 節で京都大学における Office365 Education の Shibboleth 認証連携について述べ, 4 節でこれらを総括するとともに認証システムの功罪に触れる．次いで 5 節で本稿で取り上げた事例の意義を考察し，さいごに 6 で結論として「認証基盤を制する者が大学の情報システムを制する」ことを主張し全体をまとめる．

2　群馬大学における認証の統合

2.1　認証統合のきっかけ：大学情報データベース

筆者は群馬大学総合情報メディアセンターに 2006 年 7 月に着任した．群馬大学は平均的規模の国立大学と言われており，前橋市の荒牧キャンパスに本部，教育，社会情報学部が，同じく前橋市の昭和キャンパスに医学部，生体調節研究所，医学部附属病院，桐生市に工学部があり，分散キャンパスの大学である．総合情報メディアセンターは図書館と総合情報処理センターが統合した部局で，学内の情報基盤，学術情報の整備を一元的に進める部局として誕生した．当時大学の情報公開が求められつつあり，「大学情報データベース」を構築しそれにより教員評価を行うプロジェクトが進んでいた．このような，いわば強制力のあるシステムの構築は認証の統合の契機となり，2007 年 4 月の大学情報データベース稼働時を目標に，新たな，かつ全学的な認証基盤を構築することとなった．加えて，2007 年 4 月に太田市に工学部生産システム工学科を新設することになっており，新学科の ID やメールシステムをどうするのかという問題があった．

2.2　全学認証アカウント：AXIOLE によるスモールスタート

認証基盤のデータとなるのは最低限 ID とパスワードである．新たな認証基盤を構築するにあたり，既存のキャンパスごとの ID をマージする方法，ID を天下り式に与える方法，氏名のローマ字表記を ID とする方法，職員番号を ID とする方法，ID を申請制としていわば早い者勝ちとする方法が考えられるが，ID のマージは困難であること，紙による (初期パスワードの) 通知の排除，「自分自身」で申請することに意味があるとの考えから，Web によるアカウント申請システムを構築した (図 1)．すなわち，以下の機能を実装したものであり，ユーザが申請時に入力した ID とパスワードハッシュをデータベースから AXIOLE に (手動) インポートすることで「全学認証アカウント」の登録が完了する．

- 職員番号と姓名による本人確認
- ID とパスワードは自分で決める
  - ID はメールアドレスのユーザ名部分となる
  - ID の重複がある場合は申請できない
- 申請の最終ステップで PDF が生成され申請内容を確認できる (図 2)

このように「全学認証アカウント」は当初教員と学生のみのスモールスタートであり，大学情報データベースを皮切りに，全学向け IMAP サーバ，Moodle，アルクネットアカデミーの 4 サービスをネットスプリング社の AXIOLE により認証を行う構成を取った (図 3)[6]．2007 年 4 月の教員の全学認証アカウントの教員登録率は 60% で AXIOLE のユーザライセンスは 4,000 となっていた．

図 1　「全学認証アカウントポータル」2007 年 2 月当時

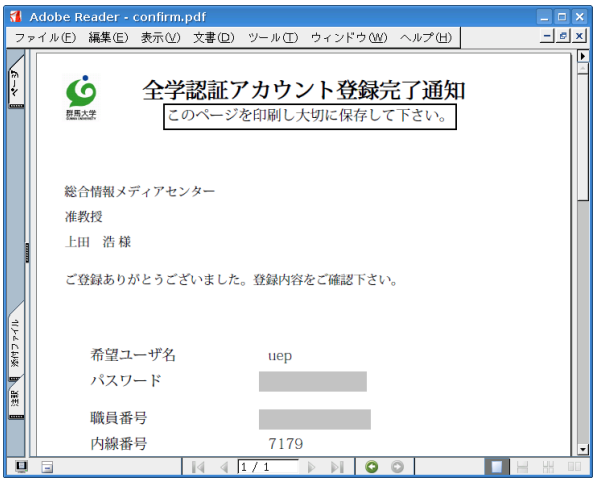

図 2　全学認証アカウント登録通知

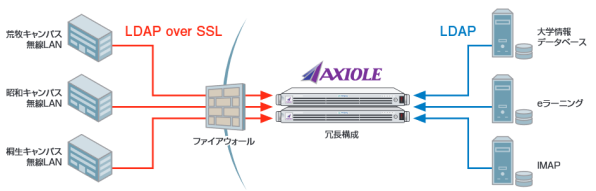

図 3　2007 年 4 月の全学認証システム概要

図 4　利用可能エリアに掲示したプロモーション用ステッカー

さらに，2008 年 3 月より学外からの PPTP VPN サービスを開始した．本サービスも AXIOLE の LDAP クライアントであるが，並行して策定していた情報セキュリティポリシーの普及を狙い，「情報セキュリティポリシー講習会」受講者のみ VPN 接続できるというインセンティブを導入した．この結果，受講者が殺到し対応が困難となった．この対応の反省をもとに，情報倫理 e ラーニングのプロジェクトが始まり今に至っている [7, 8].

これと並行し，陳腐化していた無線 LAN システムのリプレースを進め，2008 年 5 月に国立大学で初めて 802.11n 対応無線 LAN を運用開始した [6]. 本システムの運用は学内で大きなインパクトを持って迎えられた (図 4)．無線 LAN アクセスポイントは年ごとに増設していき，Aruba Networks 社の OEM 製品である Alcatel-Lucent 社の OmniAccess を採用した*1.

2.3　OmniSwitch による光直収/MAC アドレス認証ネットワークの構築

統一認証基盤の構築はキャンパスの情報化推進という大きな取り組みの一部である．2009 年 4 月に稼働する「群馬大学情報基盤システム」の調達を控え，さらなる取り組みを進めるための指針となる「群馬大学における情報化推進に向けて (総合情報メディアセンター報告)」を 2008 年 2 月に策定した．

*1 Aruba 社の製品は 1 年保証であるが，OEM の Alcatel-Lucent 社製品はメーカーの 3 年保証が付帯している．これが保守費用の削減という圧力の中 OmniAccess を採用する理由となった．

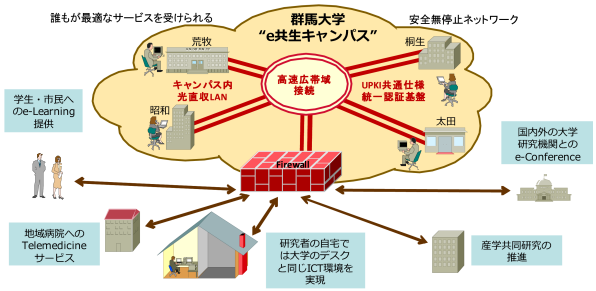

図 5　「e 共生キャンパス」と銘打ったポンチ絵

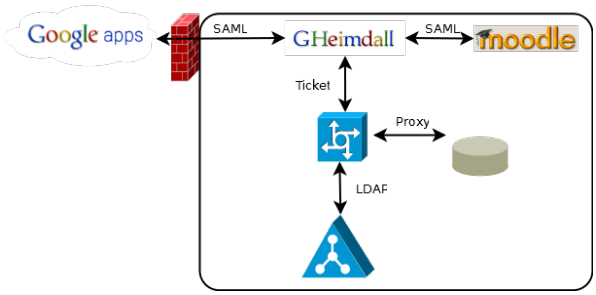

図 6　2009 年 4 月稼働の群馬大学情報基盤システムにおける認証連携

本報告は次の骨子からなり，光直収ネットワークをはじめとする先進的な取り組みを明文化し，「多様な構成員が大学の目標・目的に向かってコラボレーション (共生) できるキャンパスを目指す」ことを標榜した (図 5).

- 業務・システム最適化実現のための計画の策定
- 学内 LAN の経年故障の時期であることを指摘し「光直収ネットワーク (FTTD)」を提案，設備マスタープラン枠への応募を目指す
- キャンパスを移動すると別の ID を取得しなければならない現状を「統一認証基盤」で改善
- システムの一元化と統一認証基盤によるアクセス制御を行いセキュリティ確保のコストを集約

これらを反映したのが 2009 年 4 月に稼働した群馬大学情報基盤システムであり，4 キャンパスでバラバラであった認証基盤を統一し[*2]，Google Apps を含めたシングルサインオンを実現した (図 6).

[*2] EXGEN Networks 社の LDAP Manager を採用した.

ハードウェア面では光直収ネットワークの導入を見越し[*3]，認証 VLAN 機能の稼働実績があるアルカテル・ルーセント社の OmniSwith 9800 を採用した．ソフトウェアにおいては，サーバ系 OS に CentOS を採用するなど，オープンソースソフトウェアを導入することによりソフトウェアライセンス費用を大幅に削減した．一方，教育研究に必須のマイクロソフト社ソフトウェアは包括契約を締結し，全学認証アカウントによる認証の後ダウンロードする仕組みを構築した [9]．Google Apps によるコミュニケーション基盤は順調に稼働しており，2013 年 4 月に部局メールサーバを廃止することが決定された [10].

新システム稼働とほぼ時を同じくして，2009 年 4 月に文科省から補正予算の通知があり，設備マスタープラン枠にて応募していた光直収ネットワーク, FTTD (Fiber to the Desk) 事業の「補助金」に採択され，荒牧キャンパス学内 LAN の光直収化を進めることとなった．光直収ネットワークは基幹ルータから各部屋まで一本のファイバーで直収することで中間スイッチを排するシンプルなネットワークであり，当時千葉工業大学，埼玉大学などの事例があった．群馬大学では先行事例をさらに進め，コアスイッチ側の中間メディアコンバータじたいも排し，部屋ごとに 1Gpbs を占有できる高速化と運用負荷の軽減，利便性の向上を目指した.

FTTD ネットワークの概要図を図 9 に示す．コアスイッチは前述の通り，既存コアスイッチと合わせ Alcatel-Lucent 社 OmniSwitch 9800 を計 3 台の構成となっている．既存コアスイッチはルーティングと旧来の LAN の接続，新規追加の 2 台のコアスイッチは FTTD ネットワークの認証と VLAN へのバインドのみを行う構成とすることで，旧来の LAN からのスムーズな移行が可能になるよう配慮した．図 10 に新規追加したコアスイッチを示す．認証方式は MAC アドレス認証をデフォルトとし，MAC アドレスに対応した VLAN にバインドできるものとした．この仕組みを実現するため，ユーザ

[*3] 今だから言えるが見越して実現しなければどうしようと思っていた….

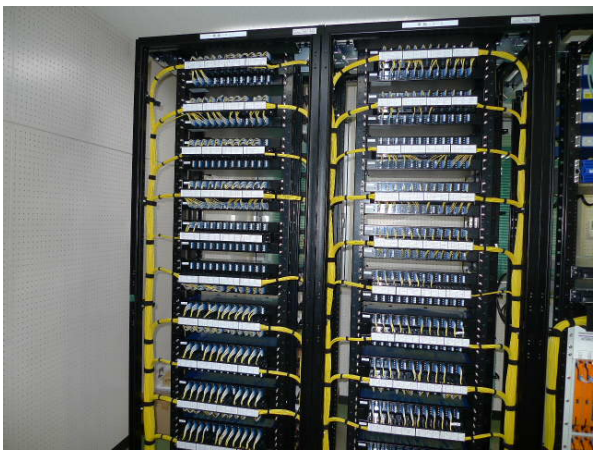

図 7　荒牧キャンパスの光ファイバーが収容されるパッチパネル:認証コアスイッチからの光ファイバーをキャンパス内の全ての部屋に配線する起点となっている．

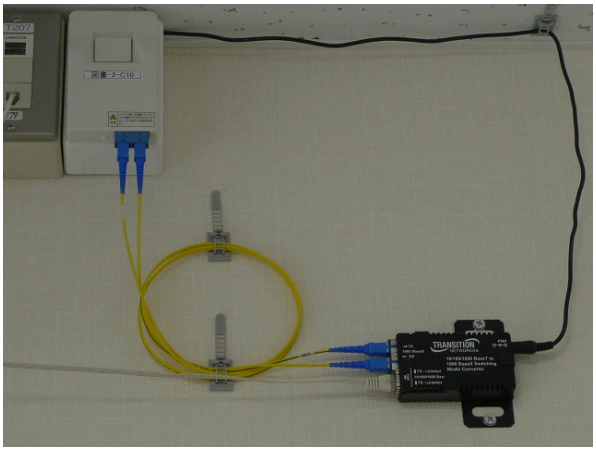

図 8　各部屋に設置されている光コンセントとメディアコンバータ: 多くの場合天井近くの壁面に設置されている．

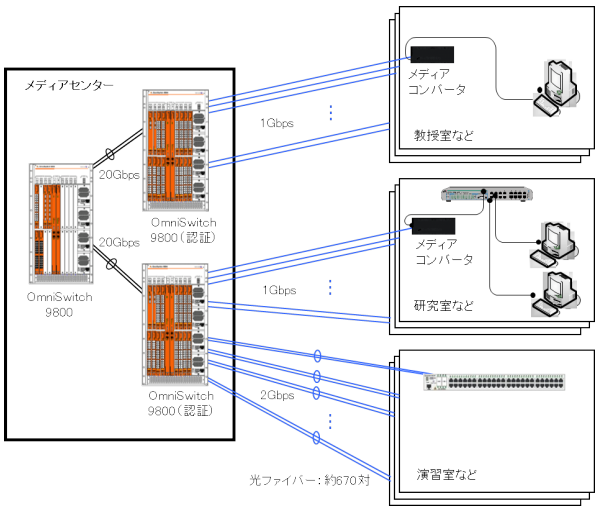

図 9　FTTD ネットワークの概要: 各部屋ごとに 1Gbps を占有できる高速ネットワークを日本で初めて実現した．

図 10　新規追加したコアスイッチ (下) と Radius サーバ (上):670 個の SFP が実装されている．既存コアとは 20G で接続されている．

が自分の機器の MAC アドレスと VLAN の対応を登録するシステムを構築した．

MAC アドレスベース認証 VLAN は図 11 に示す通り，認証スイッチ， Radius サーバ，ユーザ向け MAC アドレス登録システム，全学認証基盤が連携することで実現される．認証コアスイッチは Radius サーバに登録された MAC アドレスと VLAN の対応づけに基づいて認証成功したネットワーク機器を VLAN にバインドする． Radius サーバには FreeRADIUS を使用しており，バックエンドは MySQL である．

MAC アドレス登録システムはやはり全学認証アカウントによりログインしネットワーク機器の MAC アドレスの登録を行う．ログインしたユーザの部局情報をもとに，ユーザの所属，身分に応じたサブネット候補が表示されるようにシステムを開発した (図 12)．アドレスとサブネットの登録が完了すれば， MySQL のレプリケーション機能により，Radius サーバの MySQL に登録情報が伝搬し，

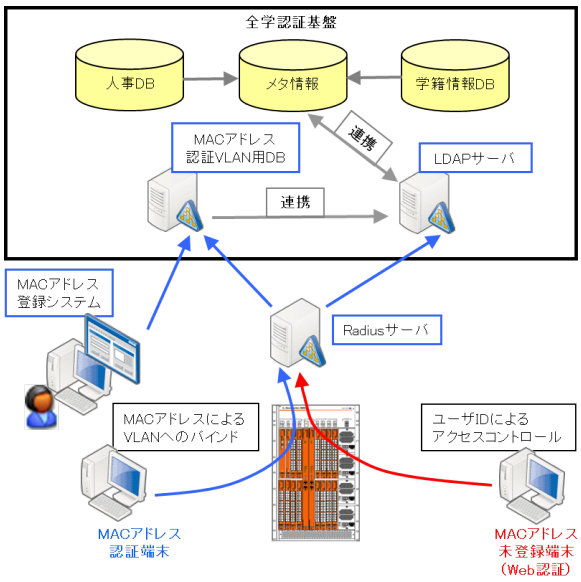

図 11　MAC アドレスベース認証 VLAN の実現手法:全学認証基盤を起点とし，MAC アドレス/ユーザ ID による認証によりネットワーク接続が可能となる．

図 12　MAC アドレス登録システム:ユーザの所属，身分に応じたサブネット候補が表示されるよう全学認証基盤との連携を行っている．

FTTD ネットワークに接続可能な状態となる．該当サブネットに DHCP サーバが存在すれば，情報コンセントに UTP で PC を接続するだけで学内 LAN を利用できる．MAC アドレスを登録していない場合，情報コンセントに PC を接続し Web ブラウザを起動すると，認証スイッチの Web インターフェースにリダイレクトされる．ここで全学認証アカウントで Web 認証の後ネットワークが利用できる．

群馬大学荒牧キャンパス FTTD ネットワークは 2010 年 3 月 23 日より運用を開始した．部屋ごとに 1Gbps を占有でき，キャンパス内であればどこでも自室 NAS やプリンタにアクセスできる環境が整った [11]．光直収ネットワークは稼働後一切の故障はないと伝え聞いている[*4]．

[*4] これはメディアコンバータを天井近くに設置するという施設部の節約プランの功績である (当時はこれが気に入らなかった)．

3　京都大学におけるクラウドサービスの認証連携

3.1　Live@edu/Office365 Education 運用の経緯

筆者が 2011 年 9 月に京都大学に異動して，まず担当したのが学生向けメールサービスのアウトソーシングである．着任した時にはすでに Microsoft のサービスを利用することは決まっていた．その経緯については [12] などを参照されたい．学生向けメールサービスは KUMOI(Kyoto University Mail clOud Interface) という公募による愛称で呼ばれ，2011 年 12 月に Live@edu によるサービスインを経て，2014 年 8 月に Office365 Education に移行しサービスを継続している．

2013 年度上半期に，すべての Live@edu 利用機関は Office365 に移行することが求められた．両者の違いを表 1 に示す．Office365 とはその名の通りメールシステムだけではなく，Office アプリケーションと情報共有のためのポータルサイト，オンライン会議，ファイル共有などのクラウドサービスを

表 1　KUMOI の仕様.

	Live@edu	Office365(Wave14)
メールアドレス	kyodai.hanako.xxx@st.kyoto-u.ac.jp	
ID	Windows Live	Microsoft Online Services
認証連携	SSO Toolkit	Shibboleth, ADFS
ライセンス	無償	有料プランあり
メールサーバー	Exchange Online（Exchenge Server 2010 相当）	
メールボックス容量	10G/アカウント	
ファイル共有	SkyDrive	SharePoint Online
メッセージング	Windows Messenger	Lync Online
組織ロゴの追加	可能	不可能
SLA	なし	有料プランのみ 99.9%

一体化した課金型のサービスであり，最も大きな違いは認証基盤とライセンスの考え方である．利用にあたり，本学では無償のプラン A2 を利用するため月額コストは不要である[*5].

システム構築/運用側にとって Office365 への移行によるインパクトが最も大きいのが認証基盤であり，ユーザ ID が Windws Live ID から Microsoft Online Services ID に変更されることにより，学内統合認証システムと Windows Live ID を同期する手順と認証連携を行う SSO Toolkit が動作しなくなることが分かった．また，これまでの Windows Live ID は削除されず残ることから，移行の際ユーザへの周知をどのように行うかについても課題があることが分かった.

認証基盤の変更に加えて，Office365 はサブスクリプションベースの製品のため，Live@edu から移行した場合にもユーザ一人一人に対し新規ライセンスの付与が必要となる．加えて，Office365 ではライセンスの付与は管理者が Web UI で行うことが想定されており，大学のように一時に多くの新規ユーザを一括登録し，同時にライセンス付与を行う業務を支援する機能がない．加えて，Office365 の Exchange Online 以外のサービスをどのように利用

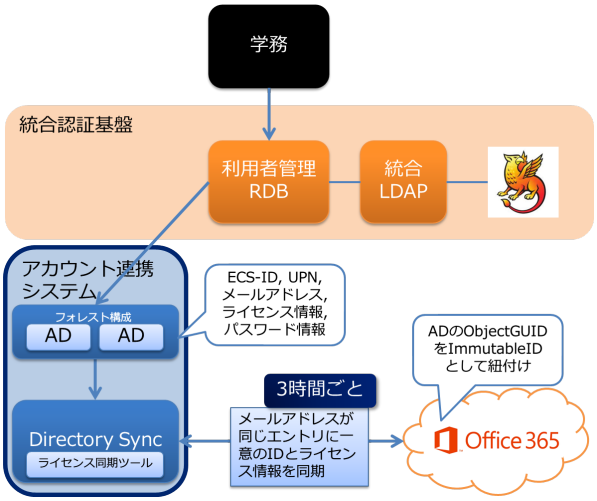

図 13　学内認証基盤とディレクトリ同期の流れ

するかという運用上の課題がある（図 15）．本学では，オンライン会議アプリケーションである Lync Online は Shibboleth フェデレーションに対応していないため，また，SharePoint は共有 Web ポータルを構築できるサービスであるが，学内の他サービスとの重複が予想されるため提供しないこととした.

Office365 ではマイクロソフトのクラウドメールシステムとしては初めて Shibboleth 連携がサポートされた．本学は様々な Web システムの Shibboleth 連携を進めており，KUMOI についてもシングルサインオンが実現できる環境が整った [13, 14]. Office365 の Shibboleth 連携は新規「アカウント連携システム」の構築により行っており，学内認証基盤と Microsoft クラウドシステム側のディレクトリ同期，ライセンス付与ツールと Shibboleth IdP を組み合わせたものである (図 13, 図 14)

我々は 2012 年夏から移行のためのシステムの検討を進め，複数回のリハーサルを行うなど周到に準備を行った．移行期間である 2013 年 8 月 19 日から 26 日の 1 週間，メール送受信のサービス自体は停止することなく継続できたことから，移行は成功したと考えられる．Office365 を Shibboleth SP として運用することにより，認証の統合を進めることができた．Live@edu での運用時は，IMAP/SMTP

[*5] その他 Office アプリケーションが利用できるプラン A3，さらにエンタープライズボイス機能（自動応答）が加わるプラン A4 がある．Office365 の利点は SLA（Service Level Agreement）であるが，無料プランについては SLA ありの記載がなく我々は混乱した．http://office.microsoft.com/ja-jp/academic/FX103045755.aspx

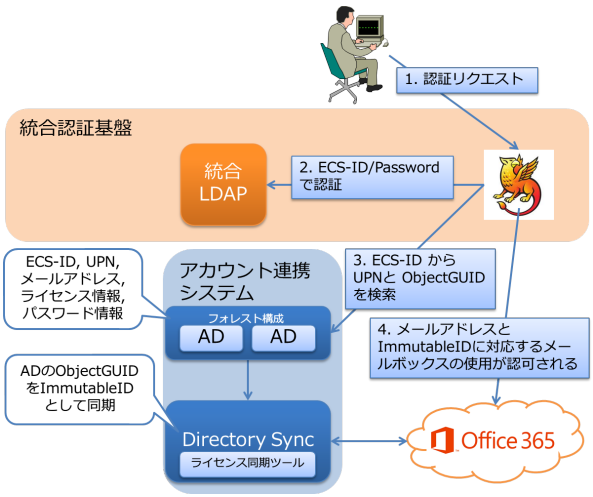

図 14　Outlook Web App 利用時の WebSSO の流れ

図 15　Office365 のライセンス上の構成.

での利用状況が全く不明であった[*6]が，Shibboleth 連携による IMAP/SMTP 利用となったことから，認証のログを取得できるようになり，より正確な利用状況の把握が可能となった.

マイクロソフトのクラウドサービスを採用し Live@edu でのサービスイン，Office365 Education への移行を経た KUMOI は，サービスを開始した 2011 年 12 月から 2015 年 3 月まで，?? 節で述べる名前解決の障害をはじめとする深刻なものが見られることを除けば，大規模障害は発生しておらず，サービスを継続することができた．図 16 に KUMOI の 2012 年 4 月から 2015 年 3 月までの「到達率」を示す．8 割ていどの学生が KUMOI を利用していることになり，全学生向けのコミュニケーションチャネルを確立することができたと言える．到達率は次の式で定義されるアカウント数の比であり，長期休暇期間は OWA へのログイン数が低くなっていることが推察できる.

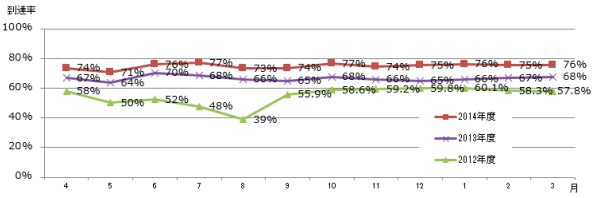

図 16　KUMOI 到達率

$$\text{到達率} = \frac{\text{該当月に OWA にログイン} \cup \text{転送設定済み}}{\text{有効な ECS-ID}}$$

3.2　Office365 Education の Shibboleth 認証連携事例の評価

残念ながら，クラウドサービスのソフトウェア側に起因する不具合が多数報告されている．問題が明らかになった日付とともに，以下に認証連携に関連するものだけを抜粋し，Office365 Education の Shibboleth 認証連携の問題点について考察する.

「Active Directory リソースにアクセスできませんでした」 本学では無効にしているグローバルアドレスリスト（以下 GAL）によるディレクトリ情報共有，AD による認証が前提のため，右クリックでメールアドレスのコピーをしようとすると「Active Directory リソースにアクセスできませんでした」などの不親切なエラーメッセージが表示される (2012 年 3 月 5 日，2013 年末サービスアップグレード後の Office365 で修正)

Live ID を直接変更できてしまう Microsoft アカウントに KUMOI のメールアドレスを設定している場合，本学認証基盤の設定同期とは関係なくバイパスしパスワード変更ができてしまう (図 17，2013 年 4 月 1 日，Office365 への移行により解消)

サービスアップグレードが祭りに Office365 への移行後すぐ，本学に対しサービスアップグレード

[*6] Exchange Online にログを蓄積する機能が実質的にないことに加え，クラウド認証となるため.

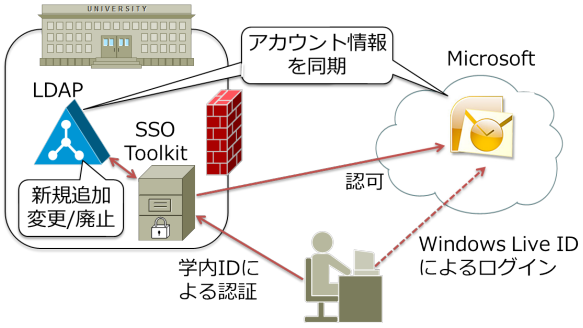

図 17　Office365 移行前の KUMOI のシステム構成．Microsoft アカウントが Live ID の場合，直接のアカウント情報編集ができてしまう．

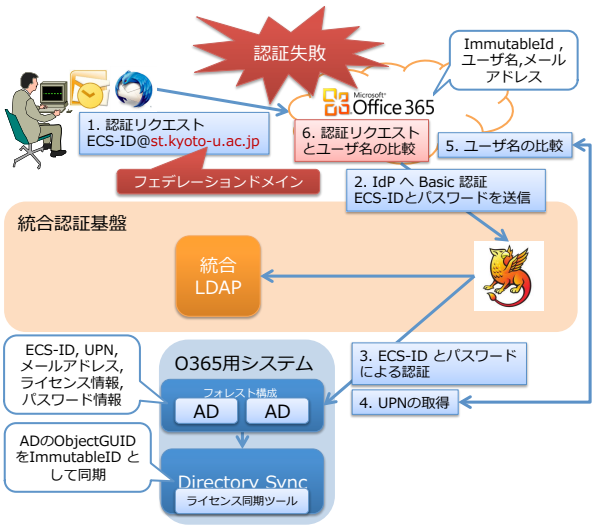

図 18　Wave15 における IMAP/SMTP 認証の流れ．「6. 認証リクエストとユーザ名の比較」で両者が一致しなければフェデレーション失敗となる．

の通知がなされた[*7]．しかしながら，Office365 への移行直後の 2013 年 9 月に，Wave15 では IMAP/SMTP クライアントとの認証シーケンスが変更され，本学のフェデレーション ID 構成では IMAP/SMTP 認証に失敗するバグがあることが判明した（図 18）．本バグはサービスの根幹にかかわるものであるため，本学テナントについてはサービスアップグレードを延期し，バグ修正が完了してからのアップグレードを行うこととなった．サービスアップグレードは 2013 年 12 月 7 日に延期された．しかしながら修正されたはずのシステムでやはり IMAP 接続ができない新たな不具合が判明し，本学認証基盤側のデータをマイクロソフト側のデータセンターに一部配信する暫定措置を行わざるを得なかった．このように，認証に関連するバグが数多く発生し続け，今だにすべてのバグが修正されたかどうか定かではない．

変わるはずのない UPN が書き換えられる (!) 前項の不具合と関連し，Wave15 へのアップグレード後，IMAP 接続時の認証リクエストのユーザ名で Office365 側 AD 内の UserPrincipalName（以後 UPN と記載）が「学内 ID@st.kyoto-u.ac.jp」で上書きされる現象が一日あたり 5〜6 件報告された．この不具合により，IMAP 接続は可能であるが OWA のみ利用できないユーザが不定数存在することになった．原因は Exchange Server 内部コードのバグであることが後に判明したが，発生条件が不明のため，毎日 UPN が上書きされているユーザを検索し元に戻すという作業を 2014 年 1 月 8 日まで毎日行わざるを得なかった．本不具合については 2014 年 1 月末から 2 月にかけて全てのサーバへ修正が行われた（はずである）．

コンプライアンストラップ？ Office ダウンロード 3.1 節で述べた通り，Office365 はメールシステムだけではない，サブスクリプションによってデスクトップ版の Office アプリケーションがダウンロードできるライセンス契約であると言え，PC に紐付くのではない柔軟なライセンス管理が可能になる意欲的なソリューションである．情報環境機構にはこれまで，「この契約で学生は Office アプリケーションが利用できるのか」「研究室で Office365 を導入したいが KUMOI との関係はどのようなものか」などと多数の問い合わせが寄せられてきた．これも，Office365 がライセンス管理ソリューションと

[*7] Wave15 と呼ばれるバージョンへの移行となる．に Live@edu から Office365 への移行したテナントでは，まず Wave14 に移行した後でなければ Wave15 へのサービスアップグレードは不可能である．

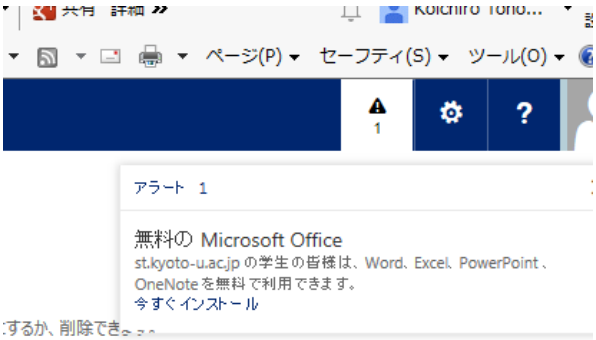

図 19　Student Advantage 対象ではない学生に「無料の Microsoft Office」と誤って表示されている．

して注目されていることの証左である．

ライセンス管理は知的財産の権利を守る重要なアクションであり，我々大学人は知的財産の扱いには慎重にならなければならない．ところが，2015 年 3 月より，学生が KUMOI にログインすると「無料の Microsoft Office」というアラートが表示されるようになった（図 19）．本来これは，（組織または部局全ての）教職員が EES/OVE-ES 契約を締結している場合，対応する学生に対し付与される「Student Advantage」と呼ばれる特典である．

調査の結果，本学では一部の部局で OVE-ES 契約が締結されているが，Microsoft の設定ミスにより，本学テナントの多くの学生アカウントに対し「Student Advantage」のライセンスが付与されていることが判明した（そもそも当該部局に対応する学生を特定することは困難なはずである）．

なお，本事象は日本の複数の大学で発生しており，各機関の管理者は一様に当惑している．我々はライセンス違反をしたかもしれない潜在的ユーザに対する Microsoft の公式回答を継続的に要求している．

以上のように，まず Office365 Education は発展途上なのか，それとも無償サービスだから期待すべきではないというレベルなのかは不明であるが品質が高いとは言えない．日本の「クオリティを追求する」文化は世界的標準から見ると厳しすぎるという見方もある．しかしながら，Microsoft がオンラインサービスを開始したのはここ数年のことではない[*8]．このような品質でこれまで Education 以外のオンラインサービスを展開してきたとすれば驚きである．また，マイクロソフトのクラウドサービスはエンタープライズ向けサービスの代替，あるいはオンプレミスシステムとの連携を前提に発展してきたものであり，どちらかと言えば企業が社員に強制的に使わせるものであることは無視できない．一方，大学におけるメールサービスは歴史があり，ユーザは愛着を持って利用している．また大学には部局ごとに様々な文化があり，Windows 以外の OS，クライアントソフトに対応しなければならず，汎用性が高い UNIX のメールシステムが使用されてきた．このような土壌の大学にはエンタープライズ向け，Microsoft 仕様，低品質ソフトウェアは適していないことが分かる．

たとえソフトウェアの不具合があっても，窓口対応によってはサービスの評価が悪くならない場合があり，サポート体制は重要である．本学ではプレミアサポート契約を日本マイクロソフトと締結し，これらの不具合や改善要望について一元的な問い合わせ対応ができる体制を整えているが，あくまで問い合わせの際のアクションが減るだけであり，質問に対する回答が明確ではない，様々な部署をたらい回しにされるという同社サポート問題点は解消されない．クラウドサービスについては，データセンターへの介入はプレミアサポートであっても困難なため，プレミアサポートが問題の解決の本質的なソリューションになっているとは言い難い状態である．

また，システム運用側がミスを繰り返すと信頼が失われ，一度失った信頼を取り戻すのは難しい．Shibboleth 認証が Live@edu 認証に勝手に変更されたインシデント [15]，パスワードポリシーなどの勝

[*8] Office365 は 2008 年からサービスを開始した Microsoft Online Services が発展したものである．

手な変更 [16]，本節で述べた Office がダウンロードできる不具合は本質的には同じことの繰り返しであり，Microsoft のシステム運用は信頼に値しないのではと愚考する次第である．

4　認証基盤整備の必要性と功罪

認証基盤整備の必要性については 2015 年の現在であれば何も説明する必要はないであろう．しかし，群馬大学で統一認証基盤構築の構想を立てた当時は技術的というより政治的事情が困難さを生んでいた．群馬大学は分散キャンパスで各学部の文化が全く異なるという典型的地方国立大学であり，認証統合を進めるにあたり，一元化してリスクも一元化するのではないかという，統合そのものに反対の声があった．そこで，認証基盤を整備するだけでなく，魅力的または強制力のあるサービスを展開するよう心掛けた．前者の代表例は無線 LAN や VPN，Microsoft 包括ライセンス契約，後者は大学情報データベースである．このような全学的サービスを展開できたのは統一認証基盤を整備することができたからである．これらの取り組みとプロモーションの結果，群馬大学総合情報メディアセンターは学内の信頼を得ることができ，サーバの学外公開申請制度，SINET 群馬ノードの桐生地区から前橋への移設など様々な改革を実行できた．これらの全ての根底にあるのは群馬大学の統一認証基盤「全学認証アカウント」であり，まさに認証を制する者は大学の情報システムを制すると言うことができる．

一方，京都大学における Office365 の Shibboleth 認証連携事例は，認証の統合が完了している状態での認証連携である．本事例にはかなりのコストが費されているにもかかわらず，ユーザへのメリットはシングルサインオンのみであり，この過程で様々な不具合が露呈した．原因は，既存の，ある意味完成した統合認証の枠組みの改修が困難であることに加え，我々がパブリッククラウドのリスクをじゅうぶんに理解していなかったこと，Microsoft のシステムが自社に閉じた環境が前提になっておりオープン系の技術と親和性が高いとは言えないことが挙げられる．クラウドサービスは一部を切り出して使用するより，すべて一体で利用できるシンプルで分かりやすいものが望ましく，残念ながら Microsoft のサービスは利用について様々なオプションがあり柔軟性が高い反面，ユーザにとっては分かりにくい．さらに，質問に対する回答が明確ではない，様々な部署をたらい回しにされるなど，Microsoft のサポート体制と初歩的なミスを繰り返したシステム運用にも改善の余地があると考えられる．

5　考察

本稿では，筆者が大学の情報サービスにインフラからコンテンツまでかかわってきた経験をもとに，「認証基盤を制する者が大学の情報システムを制する」という知見を具体的な構築運用事例を通して主張した．群馬大学における統一認証基盤の構築は魅力的なサービスの提供を標榜し，FTTD ネットワーク上の認証 VLAN に結実した．京都大学における Microsoft Office365 の Shibboleth 認証連携事例は，パブリッククラウドのリスク認識に警鐘を鳴らすものである．

LAN を認証ネットワークにすることは企業では一般的に行われているが，認証ネットワークを運用している大学は少数派である．群馬大学の事例は認証基盤の統合に加え，コアスイッチで認証を集中して行う認証ネットワークの構築運用事例としても特筆すべきものである．加えて，京都大学の Office365 と学内認証基盤の Shibboleth 認証連携事例は，オンプレミスの認証基盤をクラウドと連携することは技術的には可能であるが，実運用を行うまでには数々のハードルがあることを示唆するものである．

情報システムはその構築コストゆえに，目的に合わせ最適化されるという特性があり，認証基盤も例外ではない．ある目的の認証基盤を目的外のサービスに利用する (たとえば ID/パスワード認証のための LDAP をは職員録にはならない) ためにはそれなりのコストが必要となり，このことが，様々な大学や企業で認証基盤のスクラップ・アンド・ビルドが繰り返される要因となっている．日本ではいわゆるマイナンバーの運用が始まろうとしており，マイナ

ンバーへの対応にあたり再度の認証統合の動きがあると予想されるため，認証システムにかかわる事業者はこれまで以上にプライバシー保護に留意すべきである．

認証基盤の整備はキラーアプリケーションと一体で進めなければならない．クラウドサービスは認証基盤普及のキラーアプリになり得るが，京都大学における Office365 の Shibboleth 認証連携事例はクラウドサービスが諸刃の剣であることを示している．情報システムを「こわれもの」にしないためには，キラーアプリケーションの充実のための認証基盤の定期的なスクラップ・アンド・ビルドを行うか，十年先を見据えた拡張性の高いシステム設計が今後の課題となるであろう．

6　おわりに

群馬大学における認証の統合プロジェクト事例，京都大学におけるクラウドサービスの統合認証システムとの Shibboleth 連携事例を「認証」から俯瞰的に総括した．群馬大学における統一認証基盤の整備は，大学情報データベース，マイクロソフト包括ライセンス，VPN 接続サービス，802.11n 無線 LAN，MAC アドレス認証 VLAN など魅力的なサービスの提供を実現した．一方，京都大学における Microsoft Office365 の Shibboleth 認証連携については費したリソースにもかかわらず，様々な不具合が露呈した．Microsoft のクラウド側ソフトウェア，システム運用，サポート体制の今後の改善を期待したい．

結論として，認証基盤は大学の情報システムの要であり，その整備をキラーアプリケーションと一体で進めることが鍵である．群馬大学においては大学情報データベース, マイクロソフト包括ライセンス, VPN 接続サービス, Google Apps など強制力があり魅力的なサービスを次々とリリースしたことが成功の要因である．一方，京都大学における Microsoft Office365 の Shibboleth 認証連携については費したリソースほどにユーザにとってのメリットが感じられないものとなってしまった．クラウドサービスの利用がトレンドであるからとか，○○大学で採用しているからと思考停止するのはひじょうに危険であり，クラウド以前のサービス品質について再考すべきである．本稿が「認証基盤を制し大学の情報システムを制する」一助になれば幸いである．

謝辞

群馬大学情報基盤システムならびに FTTD ネットワークの構築運用にご尽力いただいた群馬大学総合情報メディアセンター各位，NTT 東日本各位，KUMOI の構築運用に多大なるご指導をいただいた，京都大学情報環境機構関係各位，アカウント連携システムの構築をご担当いただいたサイオステクノロジー株式会社，また技術的支援をいただいた日本電気株式会社，日本マイクロソフト株式会社各位，また様々な情報共有をさせていただいた，Office365 Education ML[*9]の皆様に厚く御礼申し挙げます．

参考文献

[1] 久長穣, 刈谷丈治, 三池秀敏：山口大学における統一認証の導入事例について, 学術情報処理研究, No. 10, pp. 55–62 (2006).

[2] 大谷誠, 江藤博文, 渡辺健次, 只木進一, 渡辺義明：シングルサインオンに対応したネットワーク利用者認証システムの開発, 情報処理学会論文誌, Vol. 51, No. 3, pp. 1031–1039 (2010).

[3] 松平拓也, 笠原禎也, 高田良宏, 東昭孝, 二木恵, 森祥寛：大学における Shibboleth を利用した統合認証基盤の構築, 情報処理学会論文誌, Vol. 52, No. 2, pp. 703–713 (2011).

[4] 高倉弘喜, 江原康生, 宮崎修一, 沢田篤史, 中村基典, 岡部寿男：安全なギガビットネットワークシステム KUINS-III の構成とセキュリティ対策 (ネットワーク管理), 電子情報通信学会論文誌. B, 通信, Vol. 86, No. 8, pp. 1494–1501 (2003).

[5] 藤村喬寿, 西村浩二, 近堂徹, 大東俊博, 田島浩

[*9] https://groups.google.com/forum/#!forum/o365edu

一, 相原玲二：スイッチベースの認証ネットワークへのシングルサインオン機能の実装と評価, 情報処理学会論文誌, Vol. 53, No. 3, pp. 958–968 (2012).

[6] 株式会社ネットスプリング：NetSpring AXIOLE 導入事例 Vol.01 国立大学法人群馬大学, http://www.axiole.jp/casestudy/jirei1.html.

[7] 上田浩, キースベアリー, 牧原功, キョクルル, 久米原栄：[招待講演] 倫倫姫プロジェクト:日英中情報倫理 e ラーニングコンテンツの開発, 電子情報通信学会技術研究報告, 第 110 巻, pp. 135–138 (2011).

[8] 上田浩, 中村素典, 古村隆明, 神智也：[招待論文] 倫倫姫プロジェクト－学認連携 Moodle による多言語情報倫理 e ラーニング－, 情報処理学会論文誌ディジタルプラクティス, Vol. 6, No. 2, pp. 97–104 (2015).

[9] 上田浩, 酒井秀晃, 青木正文, 井田寿朗, 齋藤貴英, 矢島正勝, 石原栄一, 伊比正行, 高橋仁：群馬大学におけるソフトウェアライセンス適正管理への取り組み, 平成 21 年度情報教育研究集会講演論文集, pp. D2–5 (2009).

[10] 上田浩：群馬大学における Google Apps/Gmail の導入と運用, 東京農工大学, 国立情報学研究所共催シンポジウム「キャンパス情報基盤の運営における課題と展望:学術クラウドサービス時代に向けて」, pp. 3–18 (2009).

[11] 上田浩, 井田寿朗, 青木正文, 齋藤貴英, 酒井秀晃, 伊比正行, 高橋仁, 船田博, 矢島正勝, 久米原栄：キャンパス内光直収ネットワークの構築と運用, 学術情報処理研究, No. 14, pp. 56–63 (2010).

[12] 上田浩, 上原哲太郎, 植木徹, 外村孝一郎, 石井良和, 森信介, 古村隆明, 針木剛, 岡部寿男：京都大学におけるクラウドメールサービスの運用, 大学 ICT 推進協議会 2011 年度年次大会論文集, pp. 371–373 (2011).

[13] 上田浩：Shibboleth による Office365 Education のシングルサインオン, 第 7 回統合認証シンポジウム, pp. 79–88 (2013).

[14] 上田浩, 古村隆明, 石井良和, 外村孝一郎, 植木徹：Office365 への移行と認証連携事例の評価, 大学 ICT 推進協議会 2013 年度年次大会講演論文集, pp. W3E–6 (2013).

[15] 上田浩, 石井良和, 外村孝一郎, 植木徹：Office365 Education の真実:カイゼンの裏にあるもの, 情報処理学会研究報告, 教育学習支援情報システム（CLE）, Vol. 2015-CLE-16, No. 9, pp. 1–8 (2015).

[16] 上田浩：Office365 Education のサービス品質保証契約に関する一考察, 電子情報通信学会技術研究報告, Vol. 113, No. 442, pp. 115–120 (2014).